



Department of Health and Human Services



The Centers for Medicare and Medicaid Services IT Modernization Program

Enterprise Data Center Concept of Operations for Industry

Version 1.0

October 27, 2004

This document was prepared for authorized distribution only.
It has not been approved for public release.

Executive Summary

The Centers for Medicare and Medicaid Services (CMS) have developed an information technology (IT) modernization initiative to respond to a number of environmental, programmatic, and technological drivers. This Enterprise Data Center (EDC) Concept of Operations (CONOPS) is a critical component of the modernization initiative. Implementation of the Medicare Modernization Act (MMA) has accelerated the need to successfully modernize CMS's IT environment. In many ways, the successful implementation of MMA depends on CMS's ability to develop and maintain a robust, stable, and enterprise-wide IT environment.

The breadth and impact of the MMA legislation will dramatically alter how CMS will operate in the future. It requires CMS to modernize the types and methods of delivery of health care services in the United States. One of the law's reform provisions—Medicare Fee-for-Service (FFS) Contracting Reform (MCR)—mandates that CMS must use a competitive acquisition process to transition all contracted workloads by replacing Fiscal Intermediaries and Carriers with new contractors—the Medicare Administrative Contractors (MAC). This process must begin by October 2005 and be completed within 6 years (October 2011). To facilitate these changes, CMS will need a new data center strategy and capability.

CMS IT Modernization Initiative and EDC Strategy

The IT modernization initiative will allow CMS to respond to specific environmental, programmatic, and technological drivers. Environmental drivers stem from changes in the beneficiary population and CMS's own internal staff. Programmatic drivers are the result of existing and new legislative mandates. Technological drivers derive from the increasing benefits and threats that emerging technology offers. The IT modernization initiative will help CMS:

- Reduce the time required to implement national policy changes (e.g., changes affecting provider reimbursement)
- Support e-Government mandates
- Reduce the CMS security perimeter
- Improve the capability to support increasing health care processing workloads.

The EDCs are the foundation of the enterprise infrastructure that will support a key portion of the modernization initiative. Approximately four privately owned EDCs will be operated by industry leaders. These EDCs will provide CMS with world-class application hosting centers and be capable of operating a highly redundant and scalable environment for mainframe and mid-tier computing.

The EDCs will be geographically dispersed and designed for interoperability. Toward this end, CMS will establish a common enterprise infrastructure (CEI) that facilitates highly integrated operations (e.g., cyber security), seamless handoffs between EDCs and CMS, and common reporting and management in a distributed environment.

Implementation of EDC CONOPS

This CONOPS describes the business vision of how the EDCs will support CMS and its mission. It provides a discipline-specific focus and context for the acquisition, design, development, and implementation of EDCs within CMS.

To ensure the most competitive contractual approach with industry, CMS will conduct an open competition for a multiple award, Indefinite Delivery/Indefinite Quantity (ID/IQ) EDC contract. This ID/IQ contract will provide CMS business owners with flexibility in selecting different contract types for the task orders, such as fixed unit price, cost type, or time & materials, providing maximum CMS flexibility. The EDC contract will also permit CMS to add other technology capabilities as required. It is expected that the performance-based contracts will be awarded in July 2005. Prior to award, the Office of Information Services will establish a Program Management Office (PMO) to provide a single, customer-driven focal point for CMS business owners. The PMO will serve CMS business owners and CMS external business partners, as depicted in Figure ES–1.

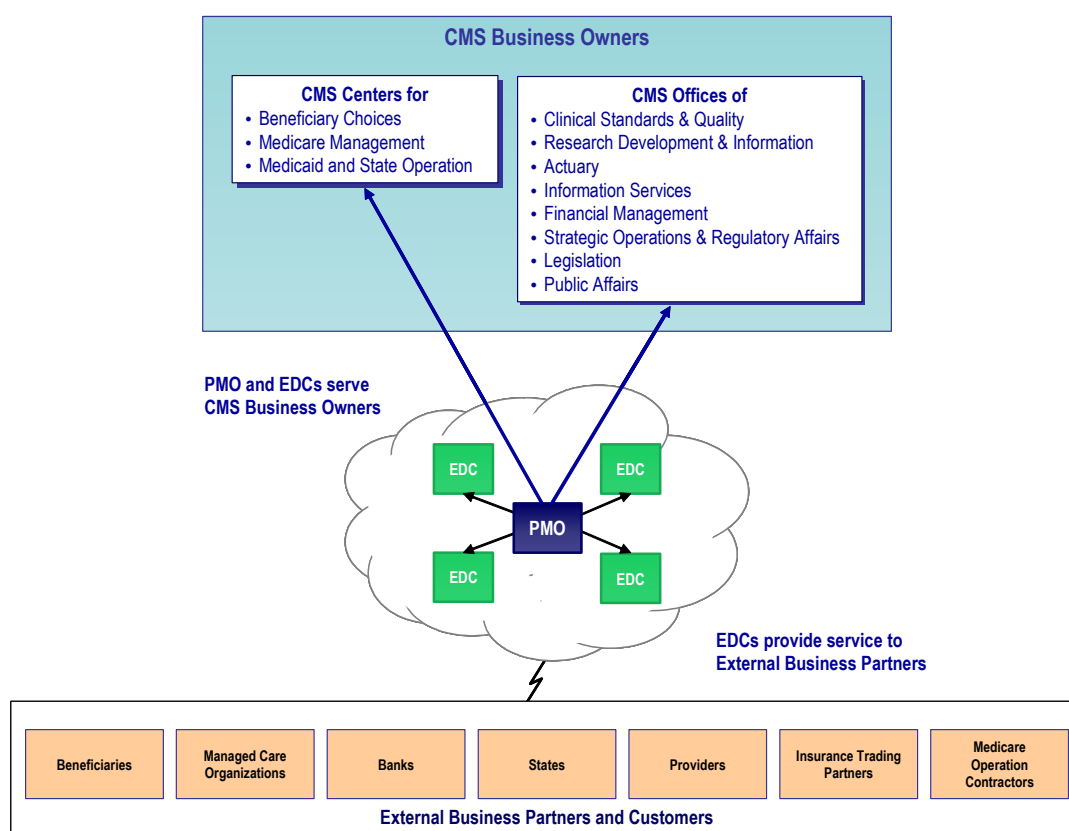


Figure ES–1. The PMO and EDCs Serve CMS Business Owners and External Business Partners

As part of the EDC Program, CMS business owners will be able to take advantage of a pre-defined process for migrating new applications or transitioning legacy applications to the EDCs.

This process will encourage competitive pricing by the EDC contractors, which will ensure that CMS and its business owners obtain best value.

Conclusion

The EDC strategy (and associated CONOPS) will provide CMS business owners with an array of benefits. These anticipated benefits include:

- Improving service levels to beneficiaries and providers through
 - Support of web-based services
 - Better and timely access to quality data
 - Relief of data center capacity constraints
 - Integrated help desks and enterprise call centers
 - Greater control over security and privacy.
- Providing CMS business owners the ability to host their applications in a CMS-controlled environment with greater flexibility to respond to increased Medicare claims processing
- Providing the computing infrastructure for Medicare Fee-for-Service Contracting Reform
- Realizing savings from economies of scale
- Improving the ability to timely implement new applications or make changes to existing applications across any EDC through the standardization of enterprise-level infrastructure.

Establishing the EDCs in a structured enterprise approach will help CMS implement its legislative mandates and best position the Agency to meet its future business needs. Through the implementation of this enterprise approach, CMS can gain greater control of data center operations, achieve greater flexibility in meeting current and future challenges, and facilitate a reduction in the number of data centers.

Table of Contents

1. Introduction.....	1
1.1 Background of Current CMS Data Center Operations	1
1.2 Problem, Issues, and Needs of the MDCs.....	2
1.3 CMS Objectives.....	2
1.4 Enterprise Data Center Strategy.....	4
1.5 Project Description.....	6
1.6 Organization of This Document.....	7
2. Elements of the EDC Concept of Operations.....	8
2.1 Purpose and Scope	8
2.2 CONOPS Overview	8
2.3 Common Enterprise Infrastructure	11
2.4 Enterprise Security Architecture.....	12
2.5 Business Continuity Planning.....	14
2.6 Program Management Office.....	15
3. CMS Application Hosting	17
3.1 Overview.....	17
3.2 New and Current Applications.....	17
3.2.1 X12N 270/271 Eligibility Inquiry and Response Transaction.....	18
3.2.2 Medicare Beneficiary Database	18
3.2.3 Calculation of True Out of Pocket Cost.....	18
3.2.4 Medicare Managed Care System	19
3.2.5 Next Generation Desktop.....	19
3.2.6 Medicare Claims Processing.....	19
4. Enterprise Data Centers.....	22
4.1 Data Center Infrastructure Architecture.....	22
4.2 EDC Operating Infrastructure Management.....	24
4.2.1 Facility Infrastructure Services	24
4.2.2 Common Enterprise-Level Infrastructure Services	26
4.3 Application Hosting and Management Services.....	31
4.3.1 Server and Mainframe Services	31
4.3.2 Storage Management Services.....	31
4.3.3 Database Management Services	31
4.3.4 Production Operations and Management Services	32
4.3.5 Configuration Management Services.....	32
4.4 Operations, Systems Engineering, and Support.....	32
Acronyms.....	33

List of Figures

Figure 1. Primary CMS EDC Stakeholders	5
Figure 2. Notional Project Description Timeline for EDC Program	6
Figure 3. High-Level View of the EDC Concept of Operations.....	9
Figure 4. Key Stakeholders in the EDC Service Life Cycle.....	10
Figure 5. Common Enterprise Infrastructure for the EDC Environment.....	11
Figure 6. EDC Three-Zone Architecture for New CMS Applications	13
Figure 7. Relationship of EDC PMO to Its Stakeholders	16
Figure 8. MDC Claims Processing Flow and Interfaces.....	20
Figure 9. Common Enterprise Infrastructure for the EDCs.....	23
Figure 10. CMS Enterprise Security Services	26
Figure 11. Enterprise Security Information and Performance Monitoring and Management System.....	29

List of Tables

Table 1. Data Center Workload by Part A, Part B, and DMERC Claims	21
Table 2. EDC Infrastructure Management Services	24

1. Introduction

The mandates of the Medicare Prescription Drug, Improvement and Modernization Act (MMA), enacted on December 8, 2003, and other recent legislation, will change the future delivery of Medicare and Medicaid healthcare services. This legislation requires the Centers for Medicare and Medicaid Services (CMS) to modernize both the types of healthcare services and the methods of their delivery. To support this modernization process, CMS needs to implement an enterprise-wide, e-Government technical information systems architecture and also provide additional data center capacity. The challenge of this change is to comply with the law without adversely impacting the delivery of healthcare services to more than 40 million Medicare beneficiaries or the many CMS business owners who are ultimately responsible for administering CMS's healthcare programs.

1.1 Background of Current CMS Data Center Operations

The CMS Data Center in Baltimore, Maryland supports the administrative and Decision Support System needs of the Agency as well as the deployment of newer MMA applications. Traditional Medicare claims are processed at 15 Medicare Data Centers (MDC) throughout the country. The estimated annual operating cost for the 15 MDCs is approximately \$250 million. The processing of Medicare claims involves 33 companies—known as Medicare Contractors—who use five different systems to process Part A claims (for hospital, skilled nursing facilities, hospice, and home healthcare services), and Part B claims (for physician, outpatient, and other ambulatory services). These Contractors consist of Fiscal Intermediaries (FI) that process Part A and certain Part B claims; Carriers that process Part B claims; and other specialized contractors—Durable Medical Equipment Regional Carriers (DMERC) that process durable medical equipment claims and Regional Home Health Intermediaries (RHHI) that process home health and hospice claims for a total of 26 FIs,¹ 18 Carriers, 4 DMERCs, and 4 RHHIs. Because some MDCs hold contracts for both Part A and Part B claims processing, CMS now maintains 54 separate contracts for this work. For the most part, CMS is two levels removed from the management and ownership of the data and claims processing information responsibilities. With the exception of MCDC1 and MCDC2 (data centers with which CMS has recently begun contracting directly), the Medicare Contractors have the sole contractual and operating responsibility with the MDCs, which has contributed to the complex nature of the pre-MMA Medicare contracting environment.

Today, the majority of CMS's data center capacity is used to support claims processing. With the enactment of the MMA and the federal government focus on e-Government initiatives, CMS is developing new applications that are driving the need for additional data center capacity with an e-Business-architected infrastructure. This additional capacity also will provide for the transition of legacy claim process applications.

¹ On September 30, 2004, as Noridian takes on the Premera Part A workload, the number of FIs will reduce to 25. The number of carriers will not change.

1.2 Problem, Issues, and Needs of the MDCs

CMS's goal is to improve the quality of service and responsiveness to the beneficiaries and providers of healthcare services. The current claims processing environment presents serious obstacles to accomplishing this goal because of the wide variations among the MDCs' capabilities and services. CMS has limited means at present to prescribe policies and procedures for ensuring the visibility, quality, and consistency of data across the MDCs. Because CMS lacks the authority to apply such controls or to effect positive change, it has encountered an array of problems with the current environment. These problems include:

- Complex contractual relationships in which CMS is one or two contract levels removed from the MDCs—namely, one level for the Carriers and two levels for the FIs
- Difficulty in imposing legislative requirements and “best practices” for system security and privacy
- Lack of CMS control and ability to coordinate enterprise-level requirements
- Complex, expensive operations
- Difficulty of providers, physicians, and practitioners in adapting to a complicated variety of preprocessing edits, reports, and support levels from the multitude of data centers
- Delayed transition and implementation of new services
- Possible loss of data when changes occur within the Medicare Contractors or MDCs
- Inability to coordinate help desk and call center operations across multiple data centers
- Lack of general control and a weakness in application controls at the MDCs.

Unless fundamental changes are made to support the management, control, and direction of claims processing, the current MDC operating environment and configuration poses enormous risks to CMS in accomplishing its current and future objectives.

1.3 CMS Objectives

CMS has adopted the following objectives to comply with the present and future legislative mandates and address its claims processing needs:

- **Reduce the lead time to implement changes in national policies.** CMS, the Congress, and providers of healthcare services are increasingly frustrated at the amount of time required to implement national policy changes that affect provider reimbursement in the Medicare program. Congress has passed legislation that would change the way in which CMS contracts for claims processing by FIs and Carriers. The Medicare Regulatory and Contracting Reform Act (MRCRA) of 2001, H.R. 3046, was approved on October 31, 2001. On December 8, 2003, President Bush signed into law the MMA;

Section 911 of the MMA establishes Medicare Fee-for-Service (FFS) Contracting Reform (MCR) that will be implemented over the next few years. This provision requires that, within 6 years (October 2005–October 2011), CMS transition all contract workloads by replacing FIs and Carriers with new contractors—the Medicare Administrative Contractors (MAC)—through a competitive acquisition process.

- **Improve CMS’s ability to support healthcare processing workload.** Claims processing is central to the success of the Medicare program and, therefore, of CMS’s mission. CMS’s mission requires promoting fiscal soundness, ensuring effective claims processing, and delivering services to beneficiaries and providers. The CMS Office of the Actuary estimates that the number of beneficiaries will increase by 15.9 percent (from 39.6 million to 45.9 million) during the coming decade (2000 to 2010). Based on historical claims data, claims volume growth will compound at 5.1 percent annually through 2005.² Any legislation that authorizes additional claims types, such as enrollment systems to support prescription drug benefits, will increase the volume of claims, potentially by an order of magnitude. Moreover, between 2010 and 2020, the post-World War II generation will become eligible for Medicare benefits,³ resulting in a 35 percent increase in the number of persons age 65 and over.
- **Implement a secure, web-based Three-Zone Architecture to support e-Government initiatives.** With the maturity of the Internet and a greater than 50 percent penetration of broadband access to small businesses and residential homes, Internet-based solutions are becoming the desired standard for commercial businesses and government agencies. These solutions greatly improve effectiveness and quality of services while providing flexibility to meet changing business needs. Internet-based solutions also offer direct access to end users, such as beneficiaries, and can significantly enhance the interaction of supply chain business partners, such as doctors and institutions. To utilize these web-enabled services, government agencies must create a secure operating environment like the CMS Three-Zone Architecture along with best-practice security solutions.
- **Reduce CMS Security Perimeter.** Fifteen MDCs currently handle Medicare claims processing in the continental United States. CMS contracts directly with two of the MDCs; the remainder are either subcontractors to the Medicare FIs and Carriers or are owned by the Medicare Contractor. The extent of the security perimeter and the different contracting arrangements make it difficult to implement and monitor common security services, intrusion detection, authentication, and encryption. The diverse platforms and operating systems (OS) also complicate the introduction of CMS standards for security architecture, configuration management, and patch management.

² The Boards of Trustees, Federal Hospital Insurance and Federal Supplementary Medical Insurance Trust Funds, *The 2002 Annual Report of the Board of Trustees of the Federal Hospital Insurance and Federal Supplementary Medical Insurance Trust Funds*, Table II.A4. Medicare Enrollment, March 26, 2002.

³ Ibid, Table V.A.2. Social Security Area Population as of July 1 and Dependency Ratios, Calendar Years 1950–2080, page 80, March 26, 2002.

The Electronic Data Processing audit of the CMS Chief Financial Officer (CFO) notes a number of vulnerabilities at the MDCs; these vulnerabilities are partially the reason for CMS's current material weakness. Although no single weakness was deemed material in the CFO's report, the aggregation of weaknesses was considered material. CMS anticipates that the number of weaknesses will decrease because of the greater ease in securing four Enterprise Data Centers (EDC), as opposed to 15 MDCs.

1.4 Enterprise Data Center Strategy

CMS is pursuing the establishment of EDCs as the most effective way to accomplish its objectives and best position the Agency to meet its business needs. Through the implementation of the EDCs, CMS can facilitate a reduction in the number of data centers, gain greater control of data center operations, and have greater flexibility in meeting current and future challenges. Through the EDC implementation, CMS will gain the capability to:

- Host applications in support of the Medicare Modernization Act
- Relieve capacity constraints at the CMS Data Center
- Deploy applications within a secure, web-based, three-zone architecture
- Provide CMS business owners the ability to migrate legacy applications to a more secure and efficient operations environment.

The anticipated benefits of the EDC strategy include:

- Improving service levels to beneficiaries and providers through
 - The support of web-based services
 - Better and timely access to quality data
 - Relief of data center capacity constraints
 - Integrated help desks and enterprise call centers
 - Greater control over security and privacy
- Providing CMS business owners the ability to host their applications in a CMS-controlled environment with greater flexibility to respond to increased Medicare claims processing
- Providing the computing infrastructure for Medicare Fee-for-Service Contracting Reform
- Realizing savings from economies of scale
- Improving the ability to timely implement new applications or make changes to existing applications across any EDC through the standardization of enterprise-level infrastructure.

A customer-driven focus is the key to the successful implementation of the EDC concept and the resulting Concept of Operations (CONOPS) described in Section 2. In recognition of the number, diversity, and complexity of the many CMS stakeholders affected by the EDCs, the Office of Information Services (OIS) will provide a Program Management Office (PMO) to give the CMS business owner a single, customer-driven focal point for use of CMS computing capabilities.

The primary CMS stakeholders that will use the EDCs to host their business applications are the three business centers responsible for delivering the Medicare and Medicaid programs at CMS—The Center for Beneficiary Choices, The Center for Medicare Management, and The Center for Medicaid and State Operations. Other CMS stakeholders that will also utilize the EDCs' capabilities are the eight CMS Offices that support the business centers and CMS as shown in Figure 1.

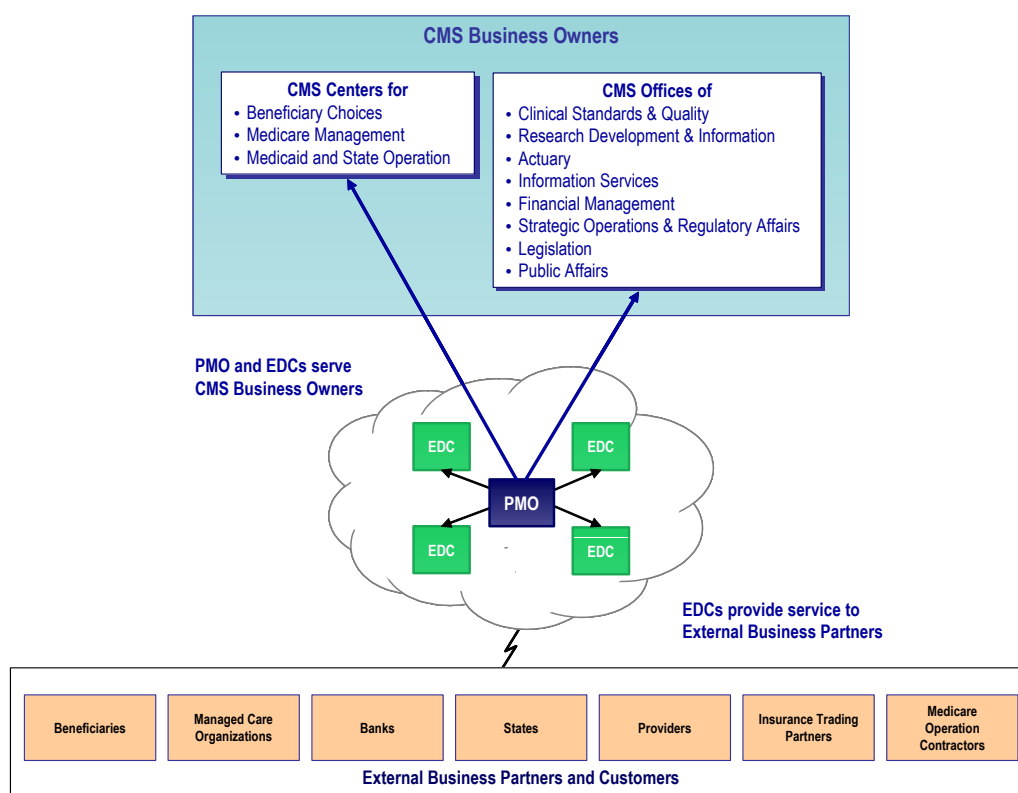


Figure 1. Primary CMS EDC Stakeholders

For purposes of this document, the CMS Centers and Offices are considered the CMS internal EDC customers, and are referred to as the “CMS business owners.” The CMS business owners will host their applications, including the necessary data processing-related support functions, at the EDCs in order to support new MMA directives and to support existing claims processing functions. Once applications are hosted at an EDC, the EDC will support the external business partners and customers who also use the CMS applications.

1.5 Project Description

The initial scope of the EDC project is to select the EDC contractors, provide the EDC infrastructure to support CMS applications, and to establish the necessary PMO and CMS processes to monitor and control the EDCs. When these EDCs are operational by the end of the third quarter of 2005, CMS business owners may deploy their applications in the EDCs. Figure 2 presents the timeline for accomplishing the major initiatives for the EDC Program.

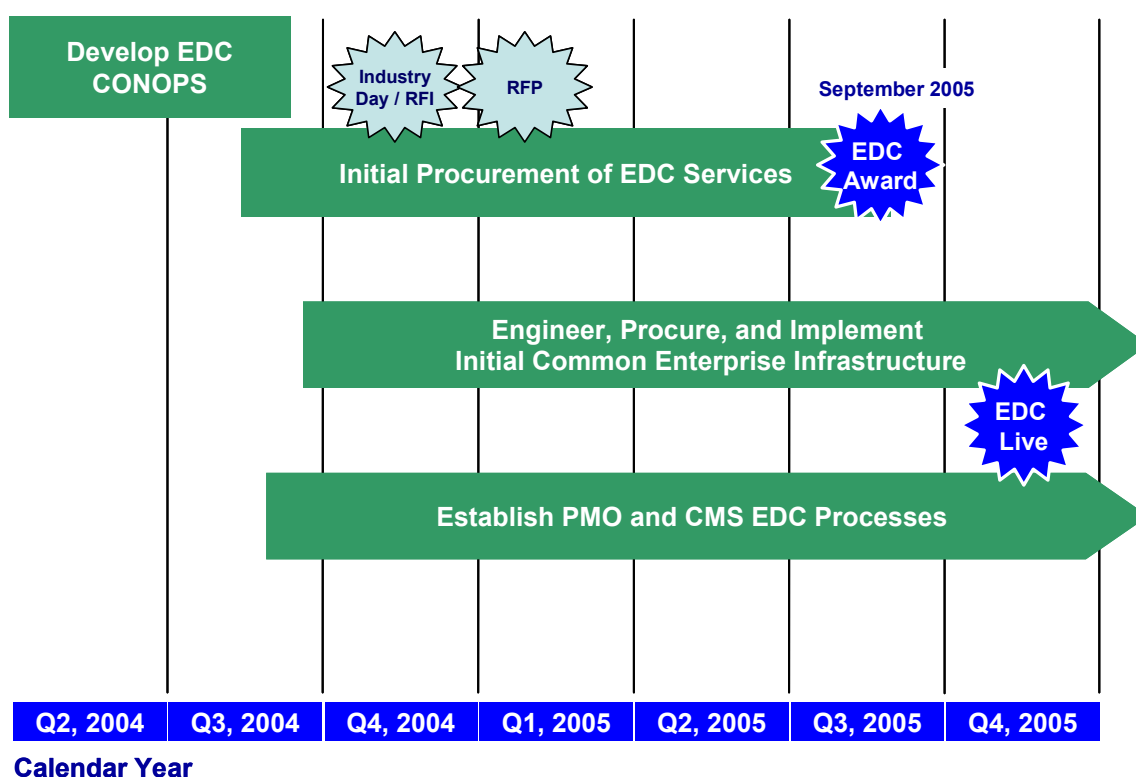


Figure 2. Notional Project Description Timeline for EDC Program

CMS has set a calendar target of mid to end of the fourth quarter 2005 for having the EDC core infrastructure and services operational. By that time, the CMS processes will be implemented to control the installation of new applications or to migrate existing applications to the EDCs. When these milestones are satisfied, application-specific tasks can be issued to the EDC contractors. The EDC contractors will then have 60–90 days to acquire and install the application-specific hardware and begin the integration testing and installation of the application.

1.6 Organization of This Document

Section 1 of this CONOPS provides an introduction of the CMS data center environment, the strategy supporting the development of the EDCs, and the current scope of the EDC project. Section 2 describes the business view of the elements of the EDC CONOPS and how the EDCs will operate within CMS. Section 3 presents an overview of the CMS applications that may be hosted within the EDCs and Section 4 defines the key operating parameters of the EDCs.

2. Elements of the EDC Concept of Operations

2.1 Purpose and Scope

The purpose of this Concept of Operations is to provide a discipline-specific focus and context for the design, development, and implementation of EDCs within CMS. The CONOPS addresses the business vision of how the EDCs will operate to support CMS and its mission. The CONOPS also delineates the operating concept and requirements of the EDC infrastructure and services.

Moving or creating a new data center within a complex business and technical environment can be fraught with risks. Unless the conception, design, and implementation is managed with a clear understanding of objectives and well-defined roles and responsibilities, the program runs the risk of cost overruns, schedule issues, and disruption to critical operations. The target (or “To-Be”) enterprise architecture must represent a well-coordinated, well-documented, and accurate representation of mission, business, services, data and information, and technology elements. Although the prescription of these architectural elements is the province of CMS’s Chief Information Officer (CIO), this CONOPS was developed to support effective coordination and collaboration with every CMS business owner.

2.2 CONOPS Overview

The EDCs should be viewed as service organizations to CMS business owners. They exist to operate systems (infrastructure and applications) that serve all of CMS’s communities, including:

- Administrative organizations
- Medicare internal and external parties
- Medicaid internal and external parties
- State Children’s Health Insurance Program (SCHIP) internal and external parties
- Health Insurance Portability and Accountability Act (HIPAA)-covered entities (Payers, Clearinghouses, Providers, etc.)
- Clinical Laboratory Improvements Amendments (CLIA) internal and external parties
- Department of Health and Human Services (HHS).

The high-level view of the EDC CONOPS, as shown in Figure 3, depicts the CMS constituents and their interactions with the EDCs and its oversight units.

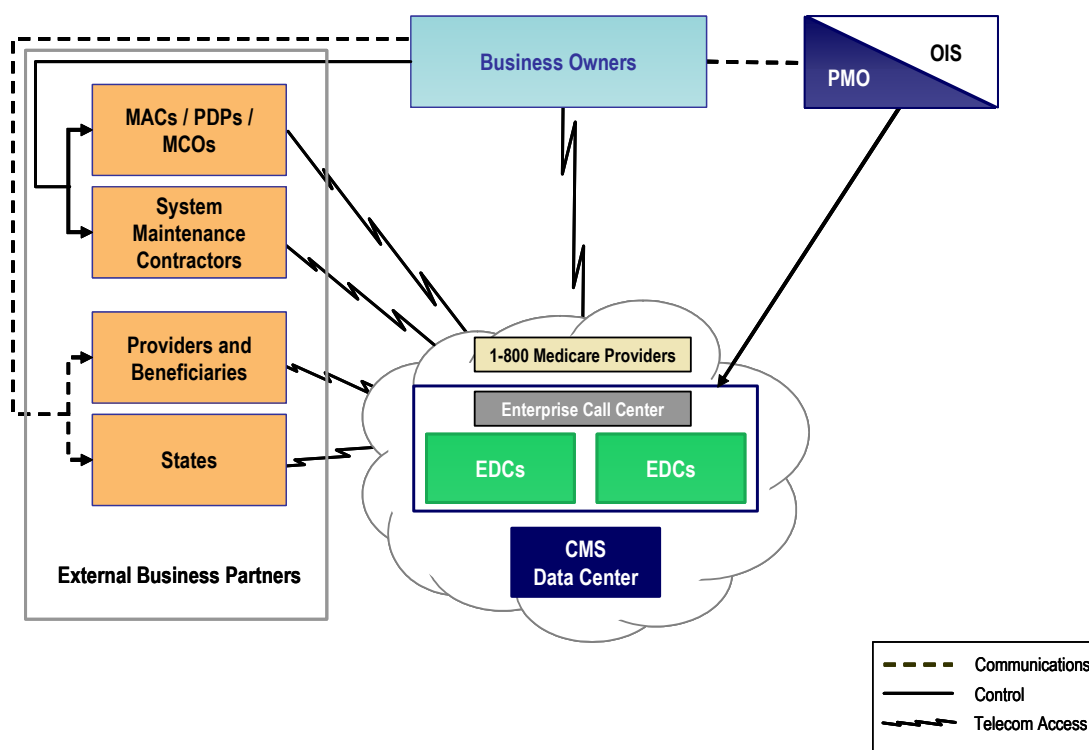


Figure 3. High-Level View of the EDC Concept of Operations

To ensure an enterprise-wide view of EDC operations, the EDCs will be managed by the CMS EDC PMO, which will operate within OIS. CMS business owners will use the PMO as the main touch point for any EDC service, although each EDC may report performance directly to an application's stakeholders. The basic business processing within each EDC—running applications, distributing reports, processing claims, supporting providers, supporting customer service centers, etc.—is not interrupted by the PMO or other organizations. The CMS business owners establish and control the interactions for basic business processes through their creation of the applications and requested services. Even though the PMO will oversee the EDCs and coordinate EDC enterprise-level activities, the CMS business owners maintain all other contractor oversight to ensure the delivery of CMS services to beneficiaries.

The CMS EDCs will have a three-phase service life cycle. As depicted in Figure 4, applications and the services for those applications are initiated upon deployment of new or modified systems. The applications reside during their life span within the EDC, and are decommissioned when the application is retired.

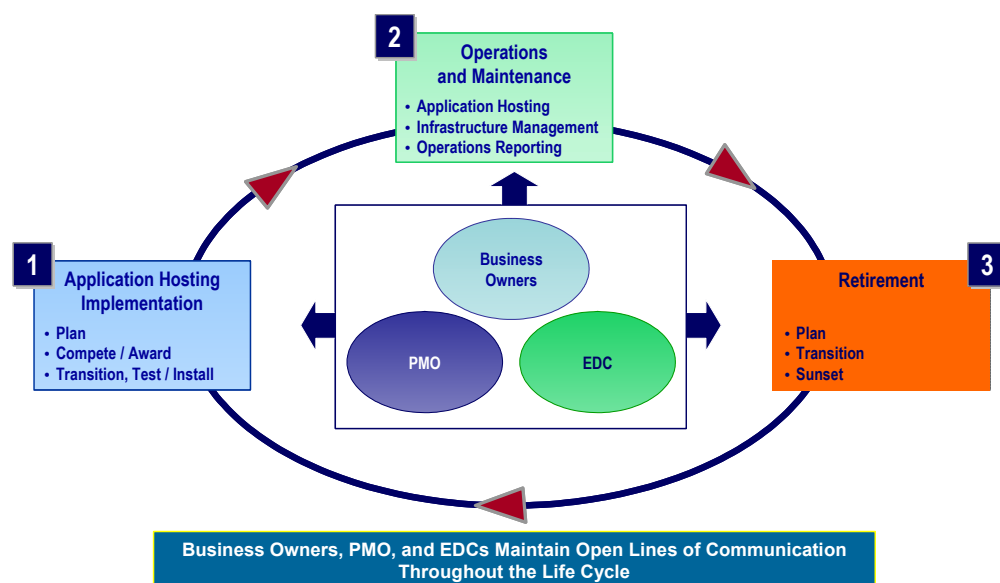


Figure 4. Key Stakeholders in the EDC Service Life Cycle

The CMS business owners, PMO, and EDC have important roles in the life cycle of applications and infrastructure management. Their distinct roles at each phase in the EDC Service Life Cycle are as follows:

- Phase 1: Application Hosting Implementation.** CMS business owners will drive the migration of new applications or the transition of existing legacy applications and will request EDC services to meet their needs; selected PMO staff will provide planning support to EDC project personnel who respond to these CMS business owner requests for application deployment or services. Deployment of applications (including migration of applications to another data center) is executed by all parties.

The PMO staff will provide the central planning point to coordinate satisfaction of the CMS business owner's needs with the system maintenance organization's tasks, the EDCs' tasks, and the service contractor (e.g., MAC or Carrier, or CMS organization) for any deployment. The PMO also maintains an overall system maintenance schedule, with each EDC tracking its deployments according to that schedule.

- Phase 2: Operations and Maintenance.** The EDC undertakes the task of deploying and executing the application and the Medicare Contractor is responsible for providing business services (customer service, claims processing support, enrollment assistance, etc.) on a day-to-day basis. The service contractor will interact as specified by the CMS business owner. All parties coordinate on problem tracking and problem resolution. The PMO ensures the customer-driven focus at all times and coordinates, as needed, the optimal leveraging of skills and resources of all parties in management of EDC performance.

- Phase 3: Retirement.** As applications are phased out, the PMO will work with the EDCs and CMS business owners to sunset the service and application. Standard operating procedures (SOP) will be developed that will guide the retirement process.

2.3 Common Enterprise Infrastructure

CMS will implement a common enterprise infrastructure (CEI) when distributed operations must be highly integrated (e.g., cyber security), where seamless handoffs between EDC and CMS operations are mandatory, and for common reporting and management. Figure 5 shows the three critical CEI platforms planned for the EDCs. Section 4, “Enterprise Data Centers,” presents a detailed discussion of these CEI platforms.

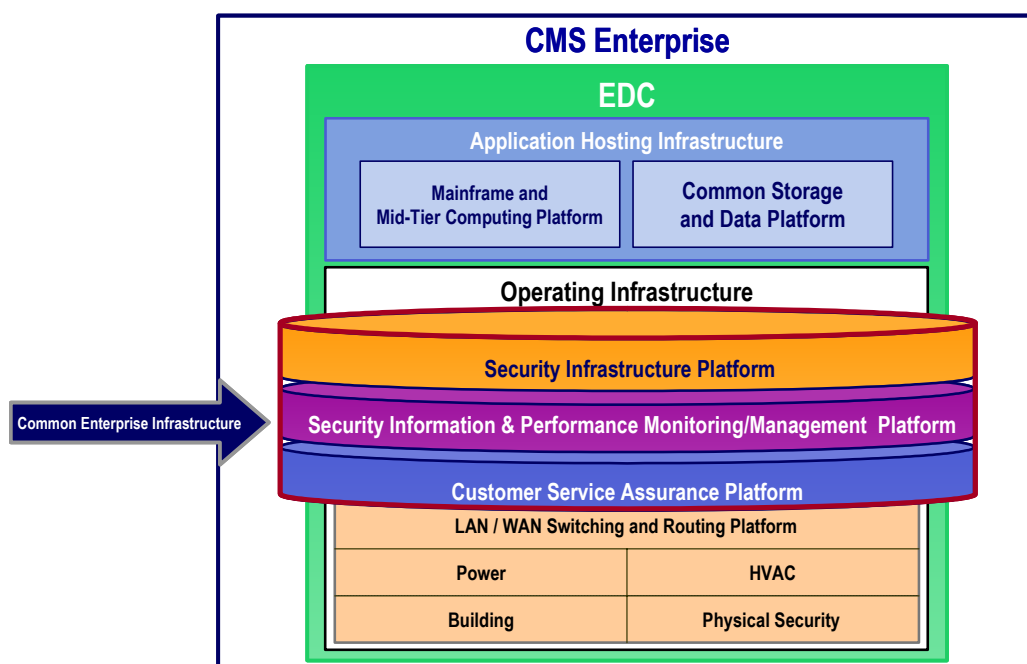


Figure 5. Common Enterprise Infrastructure for the EDC Environment

The CEI will provide CMS the degree of enterprise-level visibility, reporting, and controls to better manage the provision of healthcare services while simultaneously ensuring consistency and continuity among the EDCs. By implementing CEI, CMS can establish uniformity of information services in a distributed EDC environment.

When specific infrastructure or systems qualify as CEI, CMS will engineer the solutions to be implemented by the EDCs. These solutions may require identical applications or hardware in all locations; in other cases, the EDC contractor may be required to provide an interface to its systems to ensure that CMS has access to the system/application data.

2.4 Enterprise Security Architecture

CMS is committed to providing a secure operating environment for existing and future CMS applications. Achieving effective security by maintaining the confidentiality, integrity, and availability of data are of paramount concern to CMS. The efficient and successful implementation of enterprise-level security is a key driver of the enterprise security architecture.

The CMS security architecture will require security services that are common across all the EDCs and that can be integrated into the existing claims processing or new CMS web services environment. This enterprise security architecture enforces a common security baseline and offers long-term cost benefits. By utilizing such enterprise security services as Identification and Authentication (I&A), CMS business owners will be able to minimize the costs of redundant systems development. These cost reductions will be derived from licensing, developing, maintaining, hosting, operating, and certifying and accrediting each security service for all CMS applications. By reducing the investments in development, maintenance, and operation of application-specific security services, CMS business owners will be able to invest more resources for business application functionality. CMS can improve customer service by simplifying interactions, “hiding access control complexity” from internal and external users/customers, increasing business process efficiency through automation, and focusing on application functionality. For example, a single enterprise user account leveraged by multiple applications can minimize CMS business owner costs by reducing user account provisioning and maintenance expenditures. A single account for each user, coupled with an enterprise Role Based Access Control (RBAC) capability, eliminates the need for multiple user accounts and reduces cost for user licenses and maintenance of multiple accounts. Other enterprise security services such as encryption, security and performance monitoring, etc., also reduce the cost of these capabilities for each application business owner. CMS will be able to achieve additional savings in the Certification and Accreditation (C&A) of the EDCs as General Support Systems (GSS). Application C&A will be simplified because enterprise security services will be certified and accredited as part of the EDC. This result should also apply to legacy applications that use enterprise security services via broker applications.

To ensure CMS’s compliance with various federal statutes and requirements, all CMS Security staff, CMS application developers, and CMS EDC contractors must adhere to CMS security policies. Moreover, the enterprise security architecture must establish the EDC security foundation that will protect CMS data from threats to confidentiality, integrity, and availability.

In addition to legacy CMS claims applications, the EDCs will operate a web services environment for new CMS applications where most services for internal and external users/customers will be provided through a web interface. The EDC enterprise architecture for new applications is designed to facilitate robust security through three zones, as depicted in Figure 6 and defined in *CMS Internet Architecture (Including Minimum Platform Security Requirements—July 2003)*.

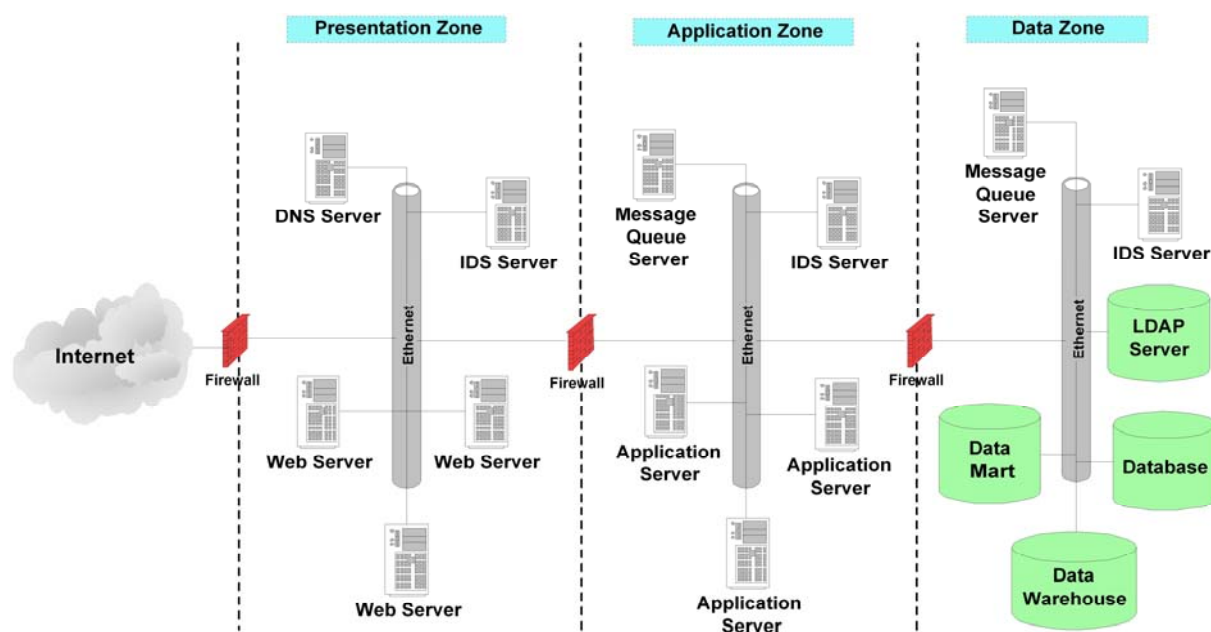


Figure 6. EDC Three-Zone Architecture for New CMS Applications

Each zone in the three-zone architecture is separated by firewalls to support web application systems. The “Presentation Zone” is the first or outermost zone. This zone supports web servers only. The Application Zone” is the second or middle zone, which supports only business logic for the applications. The “Data Zone” is the third or innermost zone, which represents the most secure or protected region of the architecture and contains the database servers used by the web applications. Additional network segments will support such specialized network services as Public Key Infrastructure (PKI), Domain Name Services (DNS), etc.

The CMS Three-Zone Architecture will support a single, unified interface for both CMS’s internal and external users/customers, as well as an operational approach to web applications developed and implemented by and/or for CMS. Applications hosted in this three-zone environment will be able to access data in the data warehouse/data marts, as well as a variety of operational databases, where and when appropriate, located within CMS and its contracted sites in the Data Zone.

The databases accessed by web applications may be on operational database servers or may reside in the data warehouse or data marts. Thus, the Data Zone will house database servers supported within CMS as well as databases accessed across all CMS. In this fashion, the Data Zone will support the secure linkage of CMS data to its internal and external users/customers.

Access to the various databases at various physical sites will be facilitated by the use of a common message-oriented interface between Application Zone servers and Data Zone servers at various sites.

The major benefits of the implementation of this three-zone architecture are to:

- Provide a standardized, secure computing environment for new CMS applications
- Provide CMS the necessary control to implement policy and requirements changes so CMS can comply with statutes and regulations on a timely basis, and to ensure the operational flexibility to handle processing reconfigurations (e.g., for workload distributions and balancing)
- Enhance the way entities interact with the EDCs by providing standard interfaces for accessing CMS applications and data (e.g., beneficiary data and claims history)
- Enable CMS to be independent, more responsive, and more effective in handling Business Operation Contractor transitions (e.g., departures or replacements).

2.5 Business Continuity Planning

CMS is responsible for the Continuity of Operations Plan (COOP) that covers the essential functions of the Medicare and Medicaid programs for meeting government-wide security and privacy standards and for protecting critical healthcare infrastructure under Homeland Security Presidential Directive (HSPD) 7.

EDCs will have business continuity capabilities that cover their operational and application requirements. A comprehensive business continuity and contingency plan (BCCP) must be established for the EDCs, and business continuity requirements must be submitted by a CMS business owner with their application deployment request. The BCCP and requirements will cover all aspects of redeploying and executing support for an application upon a major interruption of service. The plan will include disaster recovery elements of a technical and operational nature, and will address the necessary allowances for new staff, staff location changes, switching service, maintenance, and other contractors, etc. The EDC BCCP will not cover the business recovery,⁴ which is the responsibility of the CMS business owner. The detailed requirements for business continuity planning will be developed in a business continuity planning guide for EDCs.

Each EDC must support business continuity planning on two levels: first, it must comply with CMS system security requirements for external business partners, including periodic risk assessment and business continuity and contingency planning for the essential business functions of the EDC entity; second, it must support CMS business continuity and contingency planning as tasked for specific support of identified essential functions.

⁴ Business recovery includes the capability to restore the critical business environment that CMS users work in, including the offices, telephones, and computing systems to access the processing platforms. If the primary CMS business work location is not available, CMS users may be instructed to report to another CMS business work location site to perform their normal daily work functions.

Each EDC will be supporting multiple business functions with multiple owners. CMS does not expect the EDC to prioritize these functions. Rather, CMS intends to extend its set of essential functions “somewhat” and to specify to the EDCs which of the functions they support are most important.

CMS envisions that the EDCs will play a critical role in supporting CMS business continuity and contingency planning, especially once their full functionality is realized. This role may be slight at the beginning of the EDC contract, depending on the nature of the initial tasks awarded to vendors.

Ultimately, CMS expects that the EDCs will jointly support all CMS IT contingency planning, including data backup, application recovery, and disaster recovery. To the extent possible, the common infrastructure elements that are replicated in all the EDCs should enable robust and flexible support of business continuity.

2.6 Program Management Office

The PMO is CMS’s management organization responsible for oversight of the Enterprise Data Centers. The EDC PMO will serve as the customer-facing organization responsible for:

- Monitoring the EDCs’ relationships with CMS business owners and assisting the CMS business owners in using the EDCs and other CMS data center capabilities
- Providing “one-stop shopping” for EDC services and the focal point for resolution of EDC-related issues
- Oversight and program management of the deployment of new application to the EDCs, including the coordination of cost estimation and EDC management with Acquisition & Grants Group (AGG), Office of Financial Management (OFM), and the CMS business owners
- Ensuring the quality of EDC service delivery.

The PMO will be organized to support the CMS business owners’ EDC and OIS information service needs. Wherever possible, a PMO representative will be directly assigned to a CMS business owner, as shown in Figure 7, and will have total responsibility for managing the relationship with the CMS business owner as well as coordinating current and future EDC services for that business owner. The PMO will also be staffed with a group of technical and business specialists who will be qualified to support either the CMS business owner’s representative on a specific project or request or EDC requests for technical or managerial assistance. Figure 7 depicts the PMO and its relationships with its CMS constituencies.

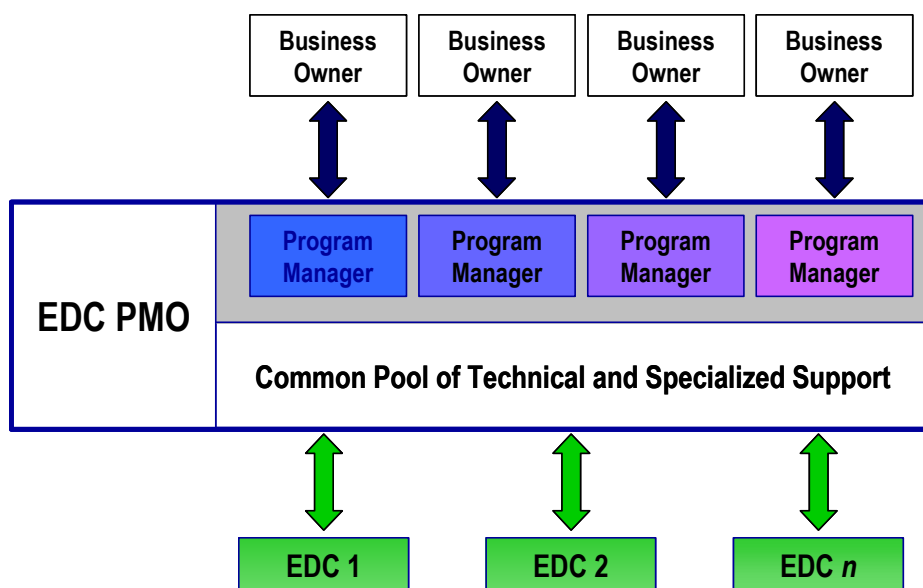


Figure 7. Relationship of EDC PMO to Its Stakeholders

The PMO will work in concert with CMS staff to facilitate the necessary actions to award a task order for hosting an application at an EDC. The PMO's responsibility to ensure the successful installation and monitoring of the EDC activities under the task order will continue throughout the life cycle of the application within the EDC. In general, the PMO will not attempt to add staff or take on tasks already executed within CMS; it will, however, coordinate these tasks. Similarly, the PMO also will not grow to handle all new tasks. If necessary, the PMO may contract for those services (such as central infrastructure management and monitoring).

The PMO will establish regulatory guidelines and measurement processes to evaluate the quality and cost performance of the EDC contractors. CMS business owners will establish the performance requirements for each application, and both the PMO and the business owner will receive reports to measure contractor performance against those expectations.

Many of the processes described at a high level in this CONOPS will be conducted by the PMO, either in concert with the EDC and CMS business owners, with other CMS departments, or in some cases independently. Organizational and procedural details for the PMO will be developed.

3. CMS Application Hosting

3.1 Overview

Once EDC operations are in place, the EDC contractors will be eligible to bid on any application that CMS business owners or OIS wish to host in the EDCs. These bids may involve new applications (or applications under development), existing CMS support applications (like email or website hosting), or the transition of existing CMS business owner applications for processing current Medicare and Medicaid claims.

The EDCs' operations, systems engineering, and support personnel (as defined in Section 4) will work closely with the PMO, CMS business owners, and application developer to plan the engineering, integration, and installation of specific applications in the EDCs. CMS envisions that the EDC contractors' responsibilities relating to application deployment will include, but not be limited to the following:

- Providing qualified EDC personnel as part of the deployment team for coordinating EDC transition activities to ensure a smooth and impact-free transition
- Implementing all EDC-related tasks, including facility- and application-specific infrastructure deployment, and establishing and monitoring the application deployment project plan
- Providing an EDC integration and test environment (EDCITE) to support pre-production verification and validation of systems to be hosted. This test environment will allow the EDC to perform load and performance validation testing prior to installing the system in the EDC production environment
- Participating in the accreditation testing of the application with the EDC, if required.

The following subsections provide a high-level description of the MMA applications that will be hosted in the EDCs and the current claim processing applications that may be candidates for migration to the EDC.

3.2 New and Current Applications

On December 8, 2003, President George W. Bush signed into law the Medicare Modernization Act of 2003. This landmark legislation provides seniors and people living with disabilities with a prescription drug benefit, as well as more choices and better benefits under Medicare. The MMA legislation, coupled with other federal e-Government initiatives, has created the need for development of new applications and modernization of CMS's supporting infrastructure. These initiatives are intended to reduce administrative costs, enhance CMS control of claims processing centers, improve standardization of claims processing and processing infrastructures, strengthen security of claims processing systems and beneficiary data, and improve economies of scale.

The applications and or programs discussed in the following subsections provide insight into the potential applications for deployment in the EDCs.

3.2.1 X12N 270/271 Eligibility Inquiry and Response Transaction

The X12N 270/271 Eligibility Inquiry and Response Transaction (HIPAA 270/271) application is a new and primary candidate for implementation in a new EDC. Medicare will remain out of compliance with the HIPAA transactions and code sets regulation until this application is implemented.

The HIPAA 270/271 is intended to be a real-time transaction for conducting an immediate check of beneficiary eligibility and coverage information, which is an expectation of providers and submitters. Currently, Institutional providers perform real-time Medicare eligibility queries, either directly or by a network service vendor connected to the FI. Because of CMS concerns about the expected transaction volume, no real-time transaction was implemented at the Carriers. In addition, two major concerns for this application are response time and security. This application will require deployment at several EDCs.

3.2.2 Medicare Beneficiary Database

The Medicare Beneficiary Database (MBD) provides a comprehensive, integrated, timely, and accessible view of beneficiary-level data necessary to support the effective and efficient management of the Medicare program. The MBD eliminates the need to develop and maintain redundant beneficiary data structures, and serves as a ready solution for many diverse Medicare business objectives. The MBD-centric environment will serve as the primary source for demographic and entitlement information throughout the CMS enterprise.

In addition to the follow-on operations and maintenance, it is anticipated that MBD will serve as an integral component in the implementation of two MMA requirements: Title I, Part D – Enrollment and Eligibility.

3.2.3 Calculation of True Out of Pocket Cost

Pending the outcome of final regulations in early 2005, CMS may create a True Out of Pocket Cost (TROOP) infrastructure based on a strategy of voluntary compliance similar to the existing coordination of benefits model. If the regulations are implemented, CMS will procure a contractor to receive enrollment and claims payment information from all plans primary and secondary to Medicare. This will establish a single point of contact between the Medicare program and employers, State Pharmacy Assistance Programs, and primary and secondary payers for enrollment and claims payment information.

Under this single point of contact option, a payer primary or secondary to a Part D plan will be required to send an enrollment file to the TROOP facilitation contractor (a contractor procured by CMS). The TROOP facilitation contractor will match the payer enrollment information to Medicare enrollment records and update the MBD with the information. The other payer enrollment file information will also be used by the TROOP facilitation contractor to match

claims payment data, which will also be submitted to the TROOP facilitation contractor. Once a claim is matched against the enrollment data, the TROOP facilitation contractor will aggregate the claim records files by the Part D plan and transmit the information.

3.2.4 Medicare Managed Care System

The Medicare Managed Care System (MMCS) focuses on beneficiary enrollment and beneficiary payment. Beneficiary calculation functions are composed of a set of systems that require an integrated redesign, development, testing, and implementation on one of the new EDCs. The MMCS currently includes the Group Health Plan (GHP), Plan Information Control System (PICS), Automated Plan Payment Systems (APPS), and the Reconsideration Case Tracking System (RECON). These systems are integrated in a monthly payment system that captures enrollment in managed care plans and calculates payments and adjustments. The current monthly payment is now nearly \$3 billion, making this the largest operational payment system running at the CMS Data Center. The MMCS will serve as the platform for the implementation of two MMA requirements: Title I, Part D and Title II – Medicare Advantage.

3.2.5 Next Generation Desktop

The objective of the Next Generation Desktop (NGD) is to enhance the services provided to beneficiaries and providers. NGD provides a standard platform to support Medicare call centers across the country with timely access to consistent and accurate information. NGD requires the support by the MDCs and or EDCs for establishing interfaces and modification of operating procedures. NGD should present only a minimal impact on EDC services because any requirements associated with NGD will be addressed in the EDC architecture review and design phase prior to development of an EDC blueprint.

3.2.6 Medicare Claims Processing

The majority of the CMS applications are housed in the 15-plus MDCs that support the processing of Medicare claims. These existing applications may or may not be migrated to the new EDCs, depending on the specific needs of the CMS business owners and the need for the applications to operate within a common architecture. Also, it may be determined that some existing applications may be moved “as is,” and will not use the three-zone E-business architecture.

At present, the claims processing environment includes:

- Front-end systems [e.g., direct data entry, electronic data interchange (EDI), and optical character recognition (OCR)]
- Back-end systems (e.g., reporting and print mail)
- Appeals systems
- Call Center applications (e.g., CustomView)

- Common Working File (CWF) hosts
- CMS-maintained software (e.g., Skilled Nursing Facility Pricer).

Figure 8 shows the current MDC claims processing flow and interfaces.

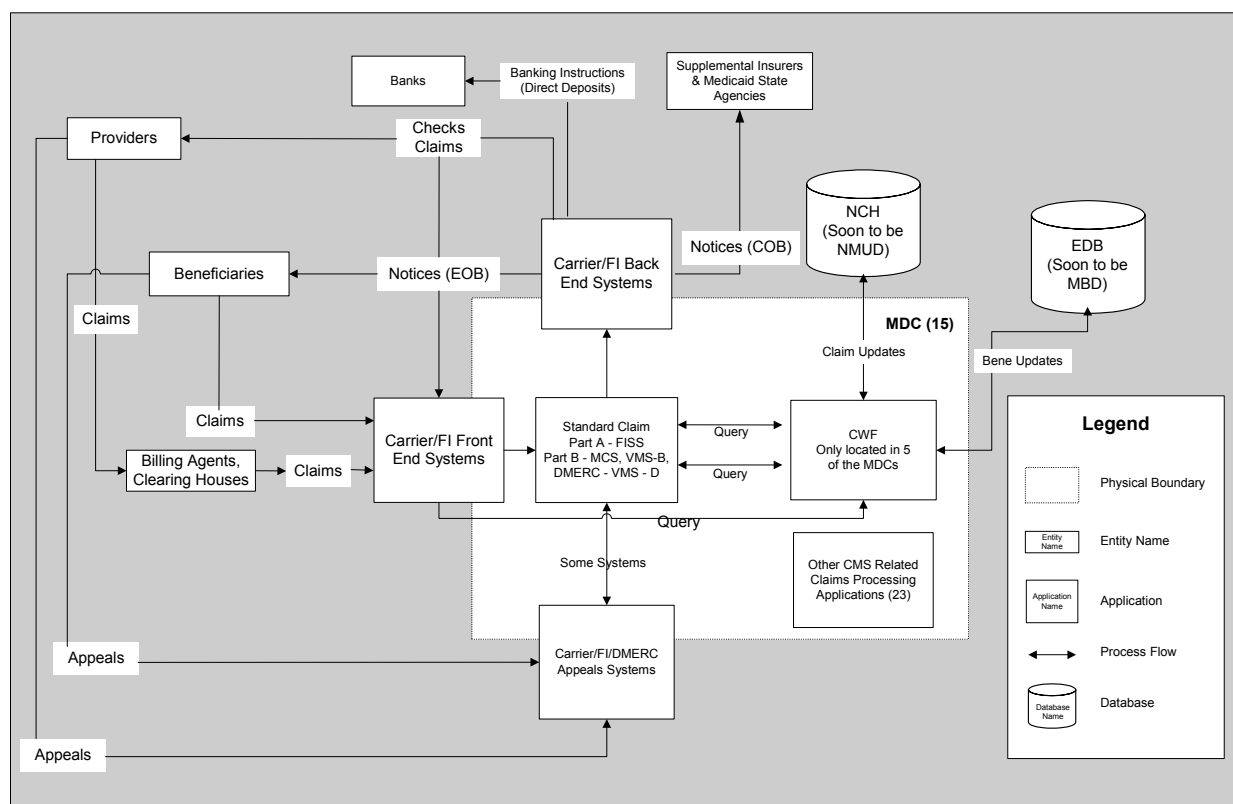


Figure 8. MDC Claims Processing Flow and Interfaces

MDC services cover a broad spectrum of support. Based on the organizational relationships, the various MDCs provide different services to the Medicare Contractors. The core services provided by MDCs include:

- **Claims Processing.** MDCs operate and manage the Shared System to process CMS Medicare claims.
- **Provide Standard and Ad Hoc Reports.** Medicare Contractors receive standard reports from the Shared Systems. The Medicare Contractors also request that the MDCs produce ad hoc reports since the MDCs control the data.

Along with their core services, some MDCs provide these optional services:

- **Host CWF.** Four MDCs host CWF under direct contract with CMS. This hosting service includes activities related to the installation, testing, and operation of the CWF.
- **Additional IT Services.** MDCs provide additional information technology services based on the needs of the Medicare Contractors and the ability of the MDCs to deliver the services. Such services include front-end processing, back-end processing, appeals processing, help desk, direct data entry, OCR, and print mail.

As a result of CMS's contractual distance from the MDCs, it has only limited ability to control the MDCs, contain processing costs, and institute required changes. The resulting claims processing environment has wide variations in the MDC services and capabilities. The resultant problems include complex, expensive operations; delayed transitions; poor security; no redundancy for disaster recovery; and possible loss of data when changes occur in the Medicare Contractors or MDCs.

Table 1⁵ presents the Data Center workload and processing requirements capacity for the estimated 2004 claims processing.

Table 1. Data Center Workload by Part A, Part B, and DMERC Claims

Type of Claim or Transaction	Total Claims (Millions)	MIPS / Mil. Claims	Estimated MIPS
Part A claims	183	20	3,660
Part B claims	864	3	2,592
DMERC claims	63	3	189
CWF transactions	1,324	0.34	450
Total MIPS			6,891

⁵ Table 1 was compiled using *Medicare Data Center Strategy Business Case Analysis* Appendices, Table M-1, Workload by Part A, Part B, and DMERC and Table M-2, Estimated Capacity Required for Claims Processing.

4. Enterprise Data Centers

The Enterprise Data Centers will provide world-class hosting services for future and existing CMS mission-critical applications of CMS business owners. These data centers will provide CMS the capability to deploy secure, scalable, high-performing applications on the Internet. The EDCs will combine “best practice” quality management systems with the best practices and secure operations found in traditional data centers with the agility, access, and customer responsiveness required for successful e-Business. By retaining the power to coordinate the performance and use of the EDCs at an enterprise level, CMS will exercise the necessary control to ensure seamless, impeccable customer service to its CMS business owners. The EDC Program Management Office within the Office of Information Services will be the focal point for coordinating and managing these data centers in accordance with this customer-driven vision.

Initially, four EDCs will be established to support the Agency’s near-term needs. The location of these data centers should be based on Medicare and other CMS services volumes, power grid separation, proximity to Internet Network Access Points (NAP), and minimization of risk from natural disasters. Under no circumstances shall two data centers be situated in the same city or geographic region.

The contracting model for the EDC work will be a multiple award, Indefinite Delivery/Indefinite Quantity (ID/IQ), hybrid performance-based task order contract. This ID/IQ contract gives the CMS business owners the flexibility to select different contract types for multiple task orders. The contract types may be fixed unit price, cost type, or time & materials. All application hosting work placed to the EDC contractors after contract award will be by way of competitive as well as directed task orders.

4.1 Data Center Infrastructure Architecture

The fundamental operating concept for the EDC infrastructure architecture will enable CMS to oversee the EDCs at an enterprise level while allowing the individual EDCs sufficient autonomy to operate a business. Enterprise-level coordination and management is a necessity where:

- **A highly integrated operating environment** is required to support a “Single Sign-On” (SSO) security approach or for managing enterprise security-level threats
- **Seamless handoffs between data centers** require such similar systems as trouble ticket resolution and tracking
- **Common reporting across data centers** is needed to for service level agreements (SLA), performance monitoring/management, and configuration management.

The key to achieving enterprise-level coordination and management requires agreement on and control of service assurance across the enterprise of data center operations, along with a set of agreed-upon EDC services and common enterprise infrastructure. Figure 9 shows the primary EDC infrastructure that will require enterprise-level engineering and deployment, and Table 2

correlates the common enterprise infrastructure (and enterprise-level management needs) to the array of EDC services. These enterprise-level systems will require standardization and will be operated in a distributed operating environment between the EDCs and CMS.

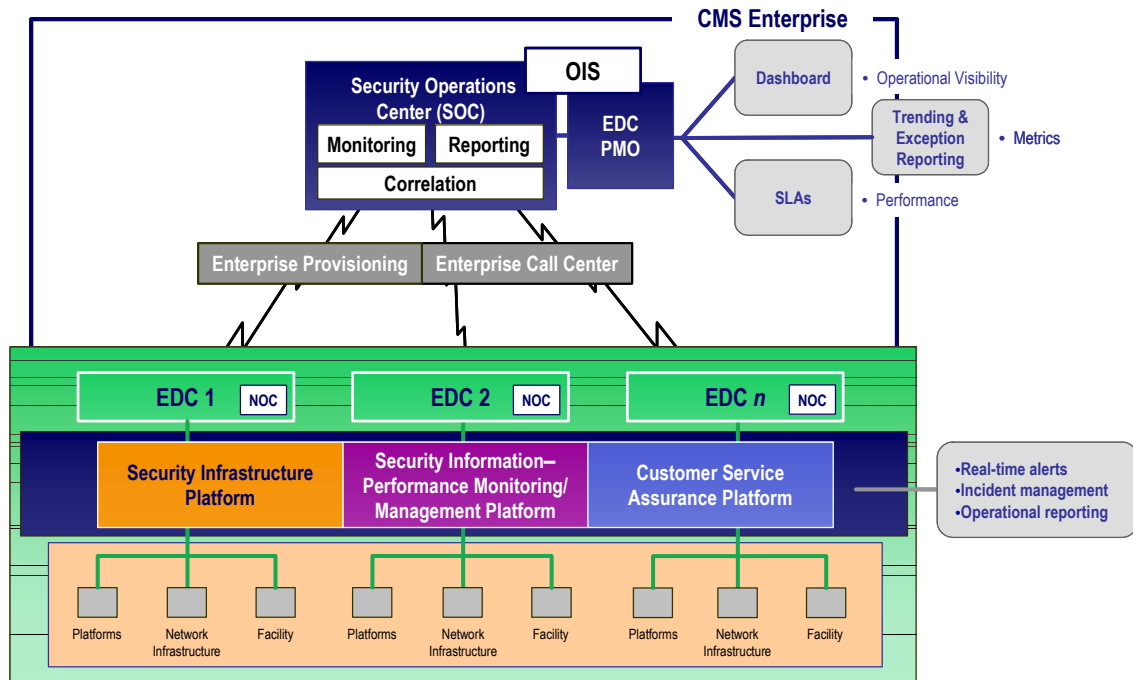


Figure 9. Common Enterprise Infrastructure for the EDCs

CMS expects the EDCs to perform as a world-class hosting data center operation, providing the necessary trusted infrastructure to support the foundation of e-Government as well as a mainframe computing environment for legacy and new large systems. The infrastructure must include consistently managed platforms that can provide high-availability, scalable, Internet-ready, tested, and proven servers and storage solutions for Microsoft WinX and Sun Solaris operating systems as prescribed by the CMS Internet Architecture.

Table 2 presents the EDC services and common infrastructure to support the existing CMS applications. The shaded cells identify the areas of CMS enterprise-level management.

Table 2. EDC Infrastructure Management Services

EDC			Infrastructure							
			Facility	Mainframe and Mid-Tier Computing Platform	Storage and Data Platform	CMS Security Platform	LAN Switching and Routing Platform	WAN Connectivity and Platform	Security and Performance Monitoring and Reporting Platform	Call Center Application and Platform
Services	Application Hosting	Server & Mainframe		X	X	X	X	X	X	
		Database Management		X	X	X	X		X	
		Database Management & Recovery		X	X					
		Configuration Management		X	X	X	X		X	X
	Infrastructure Management	Facility Management, including Physical Security and Personnel Security	X			X				
		Security Monitoring & Reporting	X			X	X	X	X	
		Performance Monitoring and Reporting				X			X	
		Help Desk	X			X			X	X
	New Services & Transition Management	Engineering and PMO Service		X	X	X	X	X	X	X

The end-state infrastructure configuration of each EDC will be determined by the CMS applications that the EDCs support; however, the goal in this EDC CONOPS is to ensure maximum flexibility to allow the EDCs to support the same applications and version across multiple EDC sites.

4.2 EDC Operating Infrastructure Management

The major EDC infrastructure and service required to support CMS's applications and information services involve facility infrastructure services; common enterprise infrastructure services; application hosting and management services; and operations, systems engineering, and support personnel. The description of these services and requirements here are not intended as a comprehensive listing, but rather as the envisioned baseline for the EDCs. Complete details of the actual requirement are specified in the EDC Acquisition Statement of Work.

4.2.1 Facility Infrastructure Services

The EDC facility will house a highly available and secure computing environment for hosting and managing CMS applications. If the facility is not totally dedicated to CMS, then the EDC contractor will provide a dedicated (not shared with other agencies or companies) and secure contiguous area for all CMS operations. The EDC shall also have a pre-production integration environment that can simulate the actual production environment to ensure the timely and seamless deployment of new services.

Providing CMS dedicated infrastructure is also required to ensure reliability, performance, and security when delivering mission-critical CMS application and services. Accordingly, other customers may not share such infrastructure as local and wide area network (LAN/WAN) connectivity, computing hardware and storage equipment, and mission-critical support systems (e.g., security). The only shared infrastructure that should be used is basic facility-related items such as power; Heat, Ventilation, and Air Conditioning (HVAC); fire suppression systems; and building management services.

Connectivity within and between the EDCs, and to the Internet, shall be capable of providing robust, redundant, reliable, and cost-effective delivery of CMS mission-critical applications. LANs within each EDC shall consist of gigabit Ethernet (GIG-E) and a dedicated switching and routing infrastructure to ensure flexible interconnectivity to all CMS devices. EDC LANs and switching/routing infrastructure will be dedicated to CMS use for security reasons. For connectivity between the EDC and the Internet, each EDC shall support an Internet Protocol (IP)-based connectivity architecture capable of running Border Gateway Protocol (BGP), Multiprotocol Label Switching (MPLS), and encrypted high-speed interconnections. Furthermore, to ensure connectivity with all CMS sites, the EDCs shall interconnect with CMS's Medicare Data Communication Network (MDCN), currently operated under contract with AT&T, and with private lines from CMS providers and/or support contractors. To manage help desk operations and inter-CMS voice traffic, the EDC shall be equipped with an IP-based PBX capable of supporting Automated Call Distribution (ACD), voice recognition (VR), and Voice over IP (VOIP).

The delivery of precise and redundant power and HVAC is critical to any data center operation. Through the service level agreement, the EDCs shall ensure a power management platform that provides:

- Local energy company power delivery across multiple power grids
- Multi-layer power generation system with conditioned AC and DC power from two independent A & B power buses
- Uninterruptible Power Supply (UPS) systems and emergency backup diesel generators
- Redundant, controlled HVAC systems that deliver constant, regulated conditioned air at precise temperature and humidity levels.

The EDC facilities as well as CMS's dedicated area shall be staffed on a 24/7/365 basis with trained security personnel to complement the automated security monitoring and surveillance systems, such as integrated closed-circuit television (CCTV) and two-factor access control (one for access to the facility and one for access to sensitive areas). All containers, briefcases, etc. shall be screened for contraband prior to entry. Visitors shall be screened upon entry to verify their identity and escorted to their destinations.

4.2.2 Common Enterprise-Level Infrastructure Services

Each EDC must be capable of operating independently and integrating with CMS for enterprise-level reporting and management in key areas of operations. The systems and or infrastructure that support these areas will be specified by CMS; each EDC will be required to run the identical software and or hardware to ensure compatibility. This top-down specification shall be required for enterprise-level coordination, reporting, and management. The key areas envisioned for this enterprise-level, top-down systems design and architecture are security systems, performance monitoring and management, and customer assurance (trouble ticket and workflow) management.

4.2.2.1 Enterprise Security Platform and Services

EDC security services will be driven at an enterprise level to create a common security environment across all EDCs. CMS will establish a security policy that will ensure a standardized security environment for CMS applications design, development, and implementation. While each CMS application is vertically integrated, the EDC infrastructure will be a horizontally shared resource among these applications. Common security services will be provided by this shared infrastructure within the EDC. For example, user I&A will be a shared service at an EDC and will be provided for new applications built to leverage enterprise security services, as shown in Figure 10.

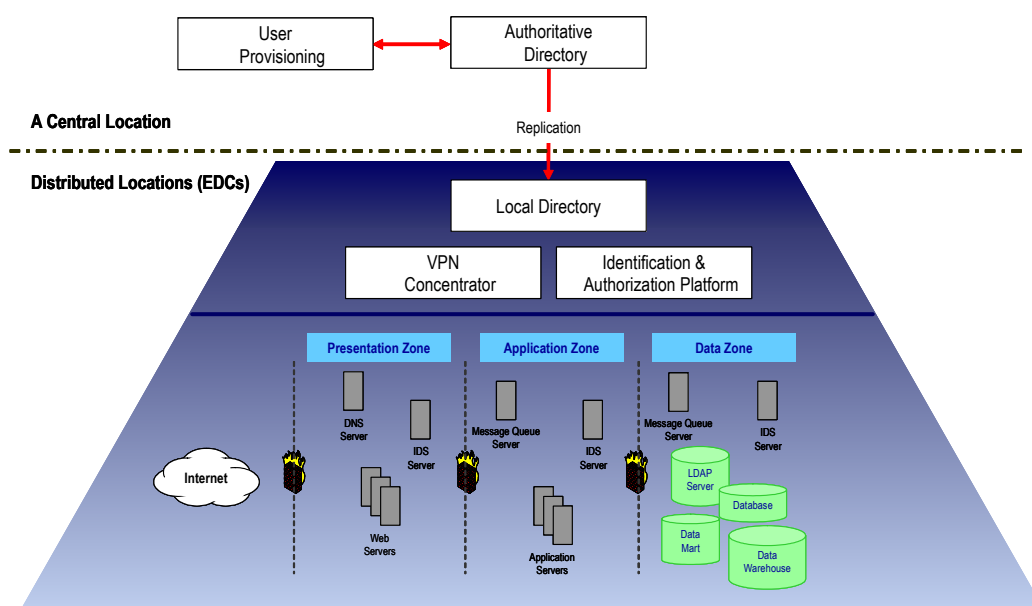


Figure 10. CMS Enterprise Security Services

CMS is subject to various federal statutes and regulations that specify systems security requirements, including the Health Insurance Portability and Accountability Act, the Privacy Act of 1974, Internal Revenue Code §6103P, the E-Government Act, the Federal Information Security Management Act (FISMA), Homeland Security Presidential Directive 7, and the Government Paperwork Elimination Act. HIPAA specifically mandates three categories of

controls to secure electronic Protected Health Information (ePHI): Administrative, Physical, and Technical.

CMS is currently developing security services guidelines that will present an overview of enterprise security services at the infrastructure level. These security services will provide the core security mechanisms for CMS applications. CMS EDCs will also provide physical security and operational security.

The actual systems architecture and engineering for CMS Security Services at both the enterprise and EDC level will be done by a third party under the direction of CMS; however, the implementation of the EDC-specific platforms and services as specified and designed will be installed and ultimately managed by the EDC contractors. The key EDC-level security platforms and systems are:

- EDC-Level Security Information Monitoring and Incident Response
- Identification & Authentication platforms
- Firewall and Intrusion Detection Systems (IDS)
- Cryptographic and Virtual Private Network (VPN) platforms.

As part of the EDC enterprise security services, the EDC contractors will be responsible for meeting CMS requirements for C&A of their data center as a General Support System. These C&A requirements include developing a System Security Plan (SSP) and Risk Assessment (RA) in accordance with CMS standards and guidelines. As part of the C&A process, the EDC contractors will also provide disaster recovery (DR) and business continuity and contingency plans based upon CMS's business continuity guidelines and CMS business owner-specific requirements. The EDCs will be responsible for developing and testing DR plans. Vulnerability assessments by independent contractors using CMS approval testing tools is an integral part of the CMS C&A process.

The EDCs shall attest to their compliance with the following requirements prior to authorization to host CMS systems or applications:

Administer Security Program

The EDC shall conduct security administration activities in accordance with the following requirements:

- The EDC complies with the security requirements defined in IOM Pub 100-17, the Business Partner System Security Manual (BPSSM), the Core Security Requirements and its operational appendices (A, B, and C), found at www.cms.hhs.gov/it/security
- The EDC adheres to all deadlines and formats outlined in official CMS communications (e.g., joint signature memorandums)
- The EDC complies with the CMS Information Security Handbook and all CMS policies, standards, and procedures contained within the handbook

- The EDC complies with the requirements for information security programs imposed on Federal agencies under the Federal Information Security Management Act of 2002, specifically the eight subsections of Section 3544(b) of Title 44, U.S. Code
- The EDC complies with and utilizes standards and guidelines promulgated by the National Institute of Standards and Technology in its entity-wide information security program
- The EDC complies with the applicable standards; implementation specifications, and requirements of the HIPAA security rule covering electronically protected health information
- The EDC fully cooperates with (including the timely installation of CMS test software on the contractor's systems) CMS audits, reviews, evaluations, tests, and assessments of contractor systems, processes, and facilities
- The EDC visits the CMS security website (www.cms.hhs.gov/it/security) at least monthly for updates to the CMS BPSSM (Publication 100-17) and related program materials and conference information.

Correct Deficiencies

The EDC shall correct any security deficiencies, conditions, weaknesses, findings, or gaps identified by audits, reviews, evaluations, and tests, including but not limited to, Statement on Auditing Standards (SAS)-70 Reviews, MMA Section 912 Evaluations and Tests, Inspector General Audits, and Vulnerability Assessments in a timely manner. Time is of the essence in correcting the deficiencies or remediating the findings of an audit.

- The EDC develops corrective action plans for any identified weakness
- The EDC corrects weaknesses within 90 days of receipt of the final audit or evaluation report
- The EDC validates and documents that corrective actions are implemented, tested, and effective.

Certification and Accreditation

The EDC shall ensure compliance with the CMS C&A methodology, policies, standards, procedures, and guidelines.

- The EDC complies with published CMS C&A methodology
- The EDC conducts or undergoes an independent evaluation and test of its systems security program in accordance with Section 912 of the MMA.

4.2.2.2 Security Information and Performance Monitoring and Management

To create a secure CMS computing environment, CMS will establish a centralized Security Information Management (SIM) system that is coupled to an enterprise-level network and platform monitoring system at a non-EDC location. The SIM will have visibility into all EDC operations and have the capability to integrate the IDS for all CMS entry points and high-value targets (HVT). Host-based IDS (HIDS) will be used to monitor designated HVTs. Network-based IDS (NIDS) will monitor both the EDC perimeter and selected HVTs. This will allow the SIM, by way of its security event and incident response capabilities within the Security Operations Center (SOC) and 24x7x365 staffing, to detect, identify, analyze, and stop enterprise-level security breaches while the EDC will manage EDC-level security issues. The SIM will also coordinate and direct specific, centralized security management services for all EDC cyber security operations, including vulnerability assessments, antivirus and firewall policies, patch distribution, event correlation and analysis, audit log analysis, and SOPs. Security configurations and corrective actions will comply with CMS policies and applicable federal regulations and legislation.

Through its allied network and platform management systems, the SIM system will also supply EDC security reporting to the EDC PMO. The integrated SIM and the Performance Monitoring/Management (PM/M) system will provide both the heartbeat and analytics of the entire EDC operations for security and network management purposes. The integrated SIM and PM/M system will also provide a proactive reporting capability of the quality of service (QoS) delivery by the EDC contractors across all EDCs. The PM/M system will deliver the data for managing all EDC contractors' SLAs and the service-level performance reports to the PMO and CMS business owners through high-level dashboards. This integrated SIM and PM/M system will be capable of monitoring such key operating performance within the EDCs as networks (e.g., switches, routers, and DNS), applications, operating systems, and storage systems as depicted in Figure 11.

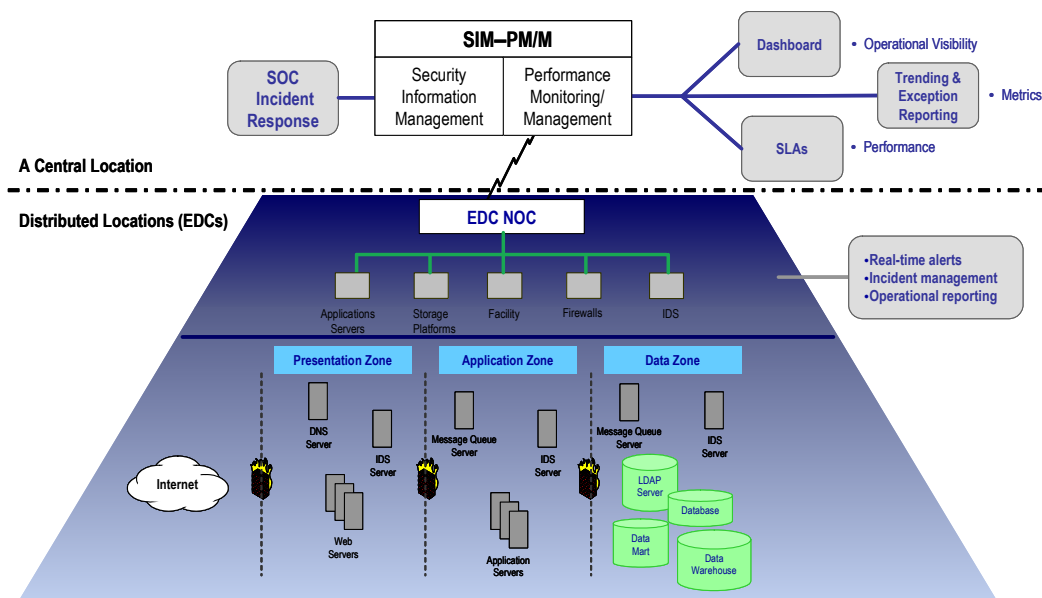


Figure 11. Enterprise Security Information and Performance Monitoring and Management System

4.2.2.3 Customer Service Assurance System and Enterprise Call Center Capabilities

A common Customer Service Assurance (CSA) trouble-ticketing and workflow management system shall be used across all EDCs to support help desk and call center functions. This approach gives CMS the ability to monitor and manage any incident irrespective of its assignment as well as facilitate the seamless transfer of any open trouble ticket to any location for resolution.

The CSA infrastructure includes a common call center utilizing a commercial off-the-shelf (COTS) application that runs on a common platform that connects to all EDCs. Through the use of a single call center system, CMS can:

- Establish a centralized call center to triage issues and distribute the call to the right EDC or CMS entity for quick resolution
- Manage escalations and severity levels
- Perform real-time exception reporting on outstanding trouble tickets
- Manage the QoS to CMS business owners by having the analytical capabilities to examine such items as recurring EDC issues, root causes, mean time to close, and first-time resolution performance
- Enforce SLAs consistently across all EDCs.

The CSA application will also provide the SOC the capability to track incidents via an incident trouble reporting system. This centralized database needs to track incidents, deficiencies, vulnerabilities, and severity levels, along with associated remedial actions, resolution dates, responsible parties, status indicators, and lessons learned from all EDCs.

CMS will establish a centralized 24x7x365 Enterprise Call Center (ECC) to triage incoming calls and determine where the call should be routed for trouble resolution. The ECC will directly interface and pass calls to all EDCs and other CMS entities. Integration of the ECC functions and workflows will be coordinated with CMS's 1-800 Medicare call center. This service will be established outside the EDC (through a separate contractor), but will use the identical CSA systems to ensure seamless handoffs.

The centralized ECC will not relieve the need for each EDC to staff a 24x7x365, technically proficient help desk capable of resolving EDC-specific issues that may affect CMS operations. The EDC help desk will be capable of resolving such issues as hardware/software availability, security incidents, application performance, and network performance. The EDC help desk will use a standard CSA system to ensure seamless handoffs and management of any call within the CMS EDCs. The EDC help desk is not intended to provide processing support of claims or questions from end users on how to use specific CMS applications or services.

4.3 Application Hosting and Management Services

Application-specific EDC hosting requirements will be provided in each new competitive task order. The task statement will specify the requirements for the application; however, it is envisioned that to qualify as an EDC contractor, each EDC must have skilled personnel with substantial experience in managing hosting services for mid-tier, web-based applications as well as for managing mainframe-based applications.

Application hosting includes the management of the full life-cycle support of an application from interfacing with application developers through integration testing and installation. Application upgrades and data center-wide integration across multiple infrastructure systems and services are included in the life cycle. Application hosting and management must include proactive monitoring and provide fault-resolution of parameters specific to the reliability of the application. The support of CMS business applications will require an array of services for servers and mainframes, storage management, database management, production operations and management, and configuration management.

4.3.1 Server and Mainframe Services

Each EDC will have the technical capabilities in product-specific hardware to support the operating systems and environments necessary to manage and tune the hardware systems used to support business applications. This includes necessary third-party hardware and technical support contracts. The actual hardware will only be required once a task order is awarded.

4.3.2 Storage Management Services

To support CMS applications, the EDC will require the use of online storage and near-line storage as appropriate. Depending on the application to be supported, Storage Area Network (SAN), Network Attached Storage (NAS), and Data Access Server (DAS) storage capabilities may be required. Storage Engineers and third-party support contracts may be required to manage the design, setup, and operation of the storage systems.

4.3.3 Database Management Services

The Database Management Services assure that the CMS data are available and recoverable. The EDC will provide for operational data management, including relational database management systems (RDBMS) and flat file data. These Database Management Services will include installation, maintenance, and customization of all database management systems (DBMS) and utilities. Database services and administrators may be required to support CMS applications for 24x7 production support, performance monitoring, capacity planning, application development integration testing, and maintenance of DBMS software.

4.3.4 Production Operations and Management Services

Production Operations and Management Services provide the daily operations activity and production control services for managing applications within the EDC. These services comprise the Run Book, executed and managed by appropriate operating system administration, database management, and media management personnel, who perform the daily delivery of data center operations. The functions included in production operations and management are:

- **Production and batch management services**, which consist of scheduling, coordination, administration, and execution of daily jobs
- **Print Services** for certain CMS services that use large-scale printers and round-the-clock operators to distribute hard copy data reports
- **Recovery Services**, such as backup and recovery (Bu/R) of data, and system configurations. The Bu/R system will handle a variety of system data, including operational data, development data, test data sets, and configurations for applications, servers, RDBMS, and network devices.
- **Media Management/Handling Services** for off-line storage and off-site storage. These services include replacing media in robots for restores, and tracking media access, location, and retention rates.

4.3.5 Configuration Management Services

Each EDC will be responsible for Configuration Management (CM); however, CMS will coordinate CM at the enterprise level for any application or common enterprise infrastructure system. A set of CM “best practices” will be agreed upon and applied by all EDCs with both the integration and production environments. Standardized security configurations shall be maintained as will a patch management program. A common CM software tool will be used to ensure consistent CM support across all EDCs. The EDC contractor will be responsible for providing a comprehensive CM and quality management function within its EDC. The CMS PMO will work with EDC contractors to develop CM and Change Control guidelines and SOPs.

4.4 Operations, Systems Engineering, and Support

Each EDC will have the necessary technical engineering capabilities to support the planning, engineering, and implementation of new applications and new infrastructure, as well as support of the enterprise-level CMS requirements. It is expected that each EDC contractor will provide a program manager to ensure a single point of contact between the EDC and the CMS Program Management Office, CMS business owners, and application developers to ensure the timely deployment of new applications. EDC contractor engineering and program management groups will not perform daily production support functions, but rather, will support new initiatives, including but not limited to, capacity planning.

Acronyms

ACD	Automated Call Distribution
AGG	Acquisition & Grants Group
APPS	Automated Plan Payment Systems
BCCP	Business Continuity and Contingency Plan
BGP	Border Gateway Protocol
BPSSM	Business Partner System Security Manual
Bu/R	Backup and Recovery
C&A	Certification and Accreditation
CCTV	Closed Circuit Television
CEI	Common Enterprise Infrastructure
CFO	Chief Financial Officer
CIO	Chief Information Officer
CLIA	Clinical Laboratory Improvements Amendments
CM	Configuration Management
CMS	Centers for Medicare and Medicaid Services
CONOPS	Concept of Operations
COOP	Continuity of Operations Plan
COTS	Commercial Off-The-Shelf
CSA	Customer Service Assurance
CWF	Common Working File
DAS	Data Access Server
DBMS	Database Management System
DMERC	Durable Medical Equipment Regional Carrier
DNS	Domain Name Services
DR	Disaster Recovery
ECC	Enterprise Call Center
EDC	Enterprise Data Center
EDCITE	Enterprise Data Center Integration and Test Environment
EDI	Electronic Data Interchange

ePHI	Electronic Protected Health Information
FFS	Fee-For-Service
FI	Fiscal Intermediary
FISMA	Federal Information Security Management Act
GHP	Group Health Plan
GIG-E	Gigabit Ethernet
GSS	General Support System
HHS	Department of Health and Human Services
HIDS	Host-Based Intrusion Detection System
HIPAA	Health Insurance Portability and Accountability Act
HSPD-7	Homeland Security Presidential Directive 7
HVAC	Heating, Ventilation, and Air Conditioning
HVT	High-Value Target
I&A	Identification and Authentication
ID/IQ	Indefinite Delivery/Indefinite Quantity
IDS	Intrusion Detection System
IP	Internet Protocol
IOM	Institute of Medicine
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Medicare Administrative Contractor
MBD	Medicare Beneficiary Database
MCO	Managed Care Organization
MCR	Medicare Fee-For-Service Contracting Reform
MDC	Medicare Data Center
MDCN	Medicare Data Communication Network
MIPS	Million Instructions Per Second
MMA	Medicare Prescription Drug, Improvement and Modernization Act
MMCS	Medicare Managed Care System
MPLS	Multiprotocol Label Switching

MRCRA	Medicare Regulatory and Contracting Reform Act of 2001
NAP	Network Access Point
NAS	Network Access Storage
NGD	Next Generation Desktop
NIDS	Network-Based Intrusion Detection System
NMUD	National Medicare Utilization Database
NOC	Network Operations Center
OCR	Optical Character Recognition
OFM	Office of Financial Management
OIS	Office of Information Services
OS	Operating System
PDP	Program Decision Package
PICS	Plan Information Control System
PKI	Public Key Infrastructure
PM/M	Performance Monitoring and Management
PMO	Program Management Office
QoS	Quality of Service
RA	Risk Assessment
RBAC	Role Based Access Control
RDBMS	Relational Database Management System
RECON	Reconsideration Case Tracking System
RFI	Request for Information
RFP	Request for Proposals
RHHI	Regional Home Health Intermediary
SAN	Storage Area Network
SAS	Statement on Auditing Standards
SCHIP	State Children's Health Insurance Program
SIM	Security Information Management
SLA	Service Level Agreement
SOC	Security Operations Center
SOP	Standard Operating Procedure

SSO	Single Sign-On
SSP	System Security Plan
TROOP	True Out of Pocket Cost
UPS	Uninterrupted Power Supply
VOIP	Voice Over IP
VPN	Virtual Private Network
VR	Voice Recognition
WAN	Wide Area Network